# CONTRACTOR REQUIREMENTS DOCUMENT

## CONTRACTOR SAFEGUARDS AND SECURITY PROGRAM REQUIREMENTS

The intent of the following requirements is that Department of Energy (DOE) contractors and their employees will adhere to the same standards for protection of materials, information, and other property of interest to the Department's Safeguards and Security Program against loss, theft, sabotage, or other hostile acts, as those required of DOE Elements and their personnel.

1. RISK MANAGEMENT. The acceptance of some level of risk is inherent in any activity. The nature of the threat, the vulnerability of the potential target, and the potential consequences of an adversarial act shall be considered in determining the appropriate level of protection against risk. Accordingly, safeguards and security programs shall be based on vulnerability/risk analyses designed to provide graded protection in accordance with the asset's importance. Risk associated with safeguards and security vulnerabilities should be reduced even where not mandated by specific requirements, when such reduction is consistent with DOE's mission and when supported by appropriate cost/benefit analyses.

2. SITE-SPECIFIC PROGRAMS. Safeguards and security programs shall be tailored to address site-specific characteristics. Site-specific protection programs shall be documented. Risks to be accepted by the Department shall be identified and documented by vulnerability/risk analyses.

3. THREAT POLICY. The Design Basis Threat Policy, issued by the Director of Security Affairs, shall be used in the design and implementation of protection programs.

4. COMPARABILITY. Safeguards and security programs shall be comparable in effectiveness to other Federally regulated programs with similar interests, when such levels are consistent with DOE protective needs and national security interests.

5. STANDARDIZATION.

   a. Safeguards and security equipment and systems shall be selected on the basis of cost savings or other benefit to DOE such as worker safety, compliance with life safety codes, enhancing mission capability, and facilitating contingency efforts.

   b. New facility designs shall incorporate the use of standardized safeguards and security equipment and systems, where possible without compromising design flexibility or adherence to performance criteria.

6. DEVIATIONS. Alternate or equivalent means of providing adequate safeguards and security may be proposed to meet a specific Safeguards and Security Program requirement, when justified. When submitting such a request, the contractor shall specify the reasons why it is

impractical or unreasonable to comply with a requirement. The following procedures and approval levels shall apply to all such deviations from requirements.

a. Variances are approved conditions that technically vary from a Safeguards and Security Program requirement, but afford equivalent levels of protection without compensatory measures.

(1) Contractors shall submit requests for variances through established channels.

(2) Variances may be approved for an indefinite period.

(3) Variances shall be documented in the appropriate safeguards and security planning documents.

b. Waivers are approved nonstandard conditions that deviate from a Safeguards and Security Program requirement that, if uncompensated, would create a potential or real safeguards and security vulnerability. Waivers therefore require implementation of compensatory measures for the period of the waiver (e.g., expenditure of additional resources to implement enhanced protection measures).

(1) Contractors shall submit requests for waivers through established channels.

(2) A waiver shall be for a period not to exceed 2 years.

c. Exceptions are approved deviations from a Safeguards and Security Program requirement that create a safeguards and security vulnerability. Exceptions shall be approved only when correction of the condition is not feasible and compensatory measures are inadequate to preclude the acceptance of risk. Contractors shall submit requests for exceptions through established channels.

(1) Exceptions shall be for a period not to exceed 3 years.

(2) The need for an exception shall be validated annually.

(3) Exceptions shall be included in Site Profiles, which form the basis for DOE's Annual Report to the President on the Status of Safeguards and Security.

d. Documentation. Specific information to be included to document each deviation is provided in Attachment 2. Approved deviations shall be documented in safeguards and security documents. A deviation request approved out of cycle with the safeguards and security plan formulation and approval process shall be documented as an attachment to the applicable safeguards and security plan.

e. Vulnerability Analyses and Performance Testing. Compensatory measures implemented and used as the basis for an exception request shall be subject to formal vulnerability assessments and must be performance tested and validated by the cognizant Field Element. The results of the vulnerability assessment(s) and performance tests shall be documented in the Site Safeguards and Security Plan. Performance testing and documentation, as necessary, may also be required for locally approved variances and waivers.

f. Validations. Cognizant Heads of Program Offices and Office of Safeguards and Security representatives may perform on-site reviews, assessments, and validation visits to ascertain the nature and impact of deviation requests.

g. Corrective Actions. Contractors shall monitor corrective actions, establish schedules, and ensure that funding is effectively managed to address safeguards and security interests and monitor compliance with schedules.

# TABLE OF CONTENTS

**CHAPTER VII - INCIDENTS OF SAFEGUARDS AND SECURITY CONCERN**



**CHAPTER VIII - CONTROL OF CLASSIFIED VISITS PROGRAM**



**CHAPTER IX - SURVEY PROGRAM**



**CHAPTER X - SELF-ASSESSMENT PROGRAM**

# CHAPTER I

## SAFEGUARDS AND SECURITY PROGRAM PLANNING

1. APPLICABILITY. This chapter applies to contractors that have responsibilities for administering and/or protecting the following sites and facilities.

   a. Those that have Category I quantities of special nuclear materials, or those that have Category II quantities within the same Protected Area that roll-up to a Category I quantity.

   b. Those that have a radiological/toxicological sabotage threat that would cause an unacceptable impact on the national security, the health and safety of employees, the public, or the environment.

   c. Those that have an industrial sabotage threat that would cause an unacceptable impact to those DOE programs supporting national defense and security.

   d. Those facilities engaged in intra-site transfer of special nuclear material.

   e. Those facilities possessing classified matter.

   f. Those facilities engaged in the protection of government property.

   g. Other facilities/sites that Heads of DOE Elements deem appropriate based on vulnerability analyses.

2. PLANNING REQUIREMENTS. The following topics shall be essential elements for planning Safeguards and Security programs.

   a. Site-Specific Characteristics. Protection programs shall be tailored to address specific site characteristics and requirements, current technology, ongoing programs, operational needs, and to achieve acceptable protection levels that cost-effectively reduce inherent risks.

   b. Threat. The "Design Basis Threat Policy for the Department of Energy (DOE) Programs and Facilities (U)" shall be used in conjunction with local threat guidance and vulnerability assessments for protection and control program planning.

   c. Protection Strategy

      (1) A denial strategy shall be used for protection of Category IA special nuclear material and radiological sabotage targets where unauthorized access represents unacceptable risk. Programs shall be designed to prevent unauthorized control (i.e., an unauthorized opportunity to initiate or credibly threaten to initiate a nuclear dispersal or detonation, or to use available nuclear materials to assemble an improvised nuclear device onsite).

(2) A containment strategy shall be used to prevent the unauthorized removal of Category II or greater special nuclear material.

(3) Should denial or containment fail, a recapture/recovery or pursuit strategy shall be employed.

(4) Programs shall be designed to mitigate the consequences of radiological/toxicological sabotage that would cause unacceptable impact to national security or pose significant dangers to the health and safety of employees, the public, or the environment.

(5) Strategies for protection and control of classified matter shall incorporate the applicable requirements established in DOE M 5632.1C-1, MANUAL FOR PROTECTION AND CONTROL OF SAFEGUARDS AND SECURITY INTERESTS, of 7-15-94; DOE M 5639.6A-1, MANUAL OF SECURITY REQUIREMENTS FOR THE CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM, of 7-15-94; and DOE M 471.2-1, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL. Emphasis shall be placed on security systems capable of detecting or deterring unauthorized disclosure, modification, or loss of classified and sensitive unclassified information and its unauthorized removal from a site or facility.

(6) Strategies for protection of government property not covered in subparagraphs (1) and (2) above shall reflect a graded approach.

(7) Security countermeasures to address bombings shall consider a range of activities from hand-carried, or mailed, to vehicle-transported devices.

d. Graded Protection Protection-related plans shall describe, justify, and document the graded protection provided the various safeguards and security interests.

3. PLANNING DOCUMENTS

a. Site Safeguards and Security Plan This plan is the master planning document that shall be prepared for sites with facilities described in paragraphs 2a, 2b, 2c, and 2d. The plan shall depict the existing condition of safeguards and security sitewide and by facility, and establish improvement priorities, and resource requirements for the necessary improvements. The plan shall contain information that describes:

(1) protection strategies;

(2) site/facility safeguards and security programs in place or planned;

(3) plans and procedures designed to implement, manage, and maintain safeguards and security programs;

(4) resources needed to sustain the site protection program in its current configuration and during planning revisions;

(5) security staff personnel qualifications as outlined in approved position descriptions and/or prescribed in DOE directives;

(6) the results of vulnerability analyses and risk assessments, including:

(a) levels of acceptable risks,

(b) assumptions established and used as part of the vulnerability analysis process, and

(c) validation of vulnerability analyses results by performance testing.

(7) required corrective actions and how they will mitigate identified vulnerabilities and reduce residual risk;

(8) sources of supporting documentation detailing where planning assumptions, relative to the facility, then adversary, and the DOE national security mission can be found; and

(9) approved deviations.

b. Security Plans. Facilities not required to prepare site safeguards and security plans shall prepare security plans that describe the protection programs in place. In addition, specialized plans shall be developed to address protection programs for classified automated information systems (AIS), materials control and accountability, and other protection operations. Requirements for these specialized plans can be found in the following directives:

(1) Materials Control and Accountability Plans. See DOE 5633.3B, CONTROL AND ACCOUNTABILITY OF NUCLEAR MATERIALS, of 9-7-94.

(2) Classified AIS Security Plans. See DOE M 5639.6A-1.

c. Planning Inputs. The following documents shall be used to support program forecasts and information input used in the protection program planning process.

(1) Current DOE directives, DOE threat guidance, and applicable intelligence assessment information developed and disseminated by Headquarters Elements.

(2) Programmatic guidance and forecasts of significant changes planned in site operations, as communicated through Heads of Field Elements and appropriate Headquarters Elements.

(3) Current and projected operational constraints and resources.

(4) Protection program policy guidance provided by DOE Elements.

d. Plan Review and Approval.

(1) Contractors shall provide Site Safeguards and Security Plans, or applicable portions thereof, to Heads of Field Elements for DOE review and approval.

(2) The Site Safeguards and Security Plan shall be reviewed and updated annually. Copies of modifications and updates shall be provided to the Head of the Field Element.

# CHAPTER II

## SAFEGUARDS AND SECURITY TRAINING PROGRAM

1. APPLICABILITY. This chapter applies to personnel performing safeguards and security tasks and responsibilities.

2. PROGRAM REQUIREMENTS.

   a. The Safeguards and Security Training Program shall encompass training in the following subjects, as applicable:

      (1) Program Management.

      (2) Personnel Security.

      (3) Protection Operations.

      (4) Materials Control and Accountability.

      (5) Information Security.

   b. Training methodology and courses shall be standardized. Development, review, and presentation of training courses for unique site-specific requirements shall be the responsibility of cognizant sites.

   c. Training programs shall be based on the results of job analyses to document the identification and description of major tasks and skill requirements.

   d. Training shall be provided to individuals to ensure they are qualified to perform assigned safeguards or security tasks or responsibilities.

      (1) Initial and refresher training shall be tailored to develop the required knowledge and skills.

      (2) The scope and level of training provided to individuals shall be tailored to their assigned duties and responsibilities and shall be based on an analysis of their prior safeguards and security experience and training.

      (3) Knowledge and performance-based testing shall apply to all required training to measure the skills acquired from the training programs developed.

(4) For specialized skill requirements, such as armorers, personnel security specialists, nuclear materials custodians, and technical security countermeasures technicians, performance testing shall form the primary basis for certification.

(5) 10 CFR, Parts 1046 and 1048, address certain specific training requirements for protective force personnel.

e. A Training Approval Program (TAP) shall be implemented to standardize safeguards and security training conducted at DOE facilities other than the Safeguards and Security Central Training Academy. (A Training Approval Program Guide will be available to provide details on training standardization.) Site programs shall be examined by Central Training Academy representatives on a recurring basis, but no less than every 3 years, to verify adherence to DOE objectives, standards, and criteria, and to provide program approval recommendations to the Director, Safeguards and Security. Training approvals shall remain valid for 3 years.

(1) Initial and recurring reviews for training approval shall cover all aspects of local training programs, including program management and structure, course contents, training facilities, observation of course presentations for effectiveness, and evaluation of students.

(2) Instructors shall be evaluated for knowledge in assigned training area and effectiveness in presenting assigned course materials.

(3) Individuals shall be tested to evaluate skills and knowledge achieved through course participation.

f. Instructors shall be certified by the individual responsible for the contractor training program. Certification shall remain valid so long as the individual fulfills applicable refresher training. Certification shall be based on a records review of qualifications and a recommendation by the individual responsible for the training program.

g. Covered contractors shall implement a standardized training records management system as described below.

(1) Records shall be maintained to document training provided to personnel participating in the DOE safeguards and security program. Records of training shall contain course identification, dates accomplished, and scores achieved, where applicable.

(2) Records of training provided to individuals shall be retained in electronic or hard copy form. Records shall be retained according to guidance provided in DOE 1324.5B, RECORDS MANAGEMENT PROGRAM, of 1-12-95, and General Records Schedules issued by the Archivist of the United States.

(a) Records of training provided at the Central Training Academy shall be maintained at the Academy and shall also be maintained by the organization sponsoring the individual.

(b) Records of training provided at DOE Elements shall be maintained at DOE Headquarters or the relevant Operations Office, as appropriate, and shall be provided to the organization sponsoring the individual for inclusion in the individual's record file.

(c) Records of training provided at contractor facilities shall be provided to and retained by the organization sponsoring the individual.

(d) Records of training provided at other government or private facilities shall be obtained and maintained by the organization sponsoring the individual.

# CHAPTER III

## PERFORMANCE ASSURANCE PROGRAM

1. APPLICABILITY. The program focus is on all safeguards and security system elements used to protect Category I and II special nuclear materials and Top Secret matter.

2. PROGRAM REQUIREMENTS.

   a. The Performance Assurance Program shall accomplish the following goals.

      (1) Provide for operability and effectiveness tests.

      (2) Be implemented in a graded manner. Elements that are determined to be most significant are "critical protection elements." Such elements shall be:

         (a) identified separately for each facility, based on consideration of the assets being protected, protection system, threat, and vulnerability assessments;

         (b) performance-tested, as a minimum, on those scenarios evaluated in vulnerability assessments;

            1 Critical protection elements shall be identified and performance tested at least every 365 days. A rationale shall be provided to characterize identified critical protection elements.

            2 Critical protection elements shall include elements and/or integrated systems of equipment and hardware, administrative procedures, protective forces, and/or other staff.

   b. Performance assurance tests shall be conducted with the highest regard for the safety and health of personnel and protection of the environment, Government property, and national security interests.

   c. The adequacy of new and existing protective systems shall be confirmed through testing prior to operational use and periodically thereafter.

      (1) Operability tests provide a simple measure of integrity on a frequent basis. Operability testing shall consist of checking the system element or total system to confirm, without any indication of effectiveness, that it is operating. Operability testing intervals may be established based on site-specific conditions and shall be documented in the performance assurance plans.

(2) Effectiveness tests provide comprehensive assurance of integrity on an infrequent basis. Performance testing of equipment for effectiveness shall consist of checking systems to confirm the satisfactory performance of the required functions over the expected range of use. The frequency of performance testing shall be appropriate to operational needs and threat levels.

d. At least every 365 days, a performance test encompassing protection systems associated with a comprehensive site or facility threat scenario shall be conducted to demonstrate overall facility safeguards and security system effectiveness.

3. DOCUMENTATION REQUIREMENTS.

a. Performance Assurance Program Plan. This plan may be an integral part of the Site Safeguards and Security Plan or other security plan, as applicable. The persons, organizations, or groups responsible for corrective actions should be identified. The Performance Assurance Program Plan shall:

(1) describe the program and its administration and implementation;

(2) identify critical protection elements and describe how the performance of these elements is to be ensured, including the manner in which activities performed by external oversight organizations will be applied and interpreted; and

(3) address unsatisfactory results of performance assurance activities, how they are to be captured in the site corrective action program, and how corrections will be implemented.

b. Performance Assurance Reports.

(1) Performance Assurance Reports shall be prepared to document results from field implementation of performance assurance activities.

(2) For evaluations based on tests or oversight activities performed by external organizations, the relevant documentation shall be interpreted and summarized or referenced.

c. Document Retention.

(1) Program and implementation plans, reports, and supporting information shall be retained as provided by law or contract, and/or as long as useful to the program.

(2) Recordkeeping systems shall be capable of providing an audit trail for performance assurance activities and reports.

(3) Disposition of documents shall be in accordance with the DOE Records Management Program.

# CHAPTER IV

## SAFEGUARDS AND SECURITY AWARENESS PROGRAM

1. APPLICABILITY. A Safeguards and Security Awareness Program shall be developed, implemented, and maintained at each facility/site/activity having DOE Security Areas, classified matter, and/or special nuclear materials.

2. REQUIREMENTS: SUMMARY OF SAFEGUARDS AND SECURITY AWARENESS PROGRAM.

   a. As a condition for unescorted access to DOE Security Areas and/or access to classified information or special nuclear materials, contractor employees (and other individuals granted DOE access authorization) shall receive briefings as required by this chapter.

   b. Individuals granted DOE access authorizations shall be precluded or restricted from access to DOE Security Areas, classified information, or special nuclear materials until the briefing requirements of this chapter have been satisfied.

   c. Briefings. Safeguards and security awareness programs shall include, but are not limited to, the development and presentation of four briefings.

      (1) Initial Briefing.

      (2) Comprehensive Briefing.

      (3) Refresher Briefing.

      (4) Termination Briefing.

   d. Topics. Safeguards and security awareness programs shall incorporate the dissemination of information concerning the following.

      (1) Applicable DOE safeguards and security regulations, directives, procedures, and guides.

      (2) Site-specific (and/or operations-specific) safeguards and security policies, procedures, and requirements.

      (3) Other matters of safeguards and security interest, such as:

         (a) recent espionage cases,

         (b) approaches and recruitment techniques employed by foreign intelligence services,

(c) safeguards or security incidents and considerations,

(d) safeguards or security threats and vulnerabilities, and

(e) classified information. If the discussion of briefing topics involves the exchange of classified information, the presentation must be limited to individuals who possess a DOE access authorization or other agency security clearance.

e. Initial Briefing.

(1) Individuals approved for unescorted access to Security Areas shall receive initial briefings.

(2) Briefing topics shall include, but are not limited to:

(a) overview of DOE safeguards and security disciplines, including personnel security, information security, and physical security;

(b) local access control procedures and escort requirements;

(c) protection of Government property;

(d) prohibited articles; and

(e) reporting of incidents of safeguards and security concern.

f. Comprehensive Briefing.

(1) Prior to being granted access to classified information or special nuclear materials, individuals granted DOE access authorizations shall receive comprehensive briefings to inform them of their safeguards and security responsibilities. When such individuals are assigned to another DOE facility, they shall receive comprehensive briefings at the new facility.

(2) Briefing topics shall include, but are not limited to, the following.

(a) Information Security.

(b) Physical Security.

(c) Personnel Security.

(d) Reporting/Notification Requirements.

(e) Legal and administrative sanctions imposed for incurring a security infraction or committing a violation.

(f) General information concerning the protection of special nuclear materials.

g. Refresher Briefings. Individuals who possess DOE access authorizations shall receive refresher briefings to reinforce and update awareness of safeguards and security policies and their responsibilities. Refresher briefings are mandatory for all individuals possessing DOE access authorizations and shall be implemented each calendar year at approximately 12-month intervals.

h. Termination Briefings. Individuals shall receive termination briefings to inform them of their continuing security responsibilities after their access authorizations are terminated. A termination briefing shall be implemented on the individual's last day of employment, the last day the individual possesses an access authorization, or the day it becomes known that the individual no longer requires access to classified information or special nuclear materials, whichever is sooner. Termination briefings shall be based on the information contained in DOE F 5631.29, "Security Termination Statement," and Standard Form 312 (SF-312), "Classified Information Nondisclosure Agreement."

i. Safeguards and Security Awareness Coordinator. The contractor shall appoint a Safeguards and Security Awareness Coordinator who shall formulate and/or maintain a safeguards and security awareness program.

3. DOCUMENTATION REQUIREMENTS.

a. Recordkeeping. Records shall be maintained in a manner that identifies all individuals who have received briefings by type and date of briefing and calendar date. Recordkeeping systems shall be capable of providing an audit trail.

b. Documentation.

(1) A completed SF-312 may serve as the documentation for the comprehensive briefing.

(2) In recurring requirements, such as the refresher briefing, records shall be maintained until the next occurrence of the briefing.

(3) The completion of DOE F 5631.29 satisfies documentation requirements for the termination briefing.

# CHAPTER V

## FACILITY CLEARANCES AND REGISTRATION OF SAFEGUARDS AND SECURITY ACTIVITIES

1. APPLICABILITY. This chapter applies to safeguards and security activities involving access authorizations, classified information, nuclear or other hazardous material that presents a potential radiological or toxicological sabotage threat, and/or Departmental property with a value of $5,000,000 or more.

2. REQUIREMENTS: GENERAL.

   a. Nuclear and other hazardous materials presenting a potential radiological or toxicological sabotage threat, classified matter, and property protection interests shall not be permitted on premises occupied by the Department or its contractors until facility clearance is granted.

   b. Safeguards and security activities involving access authorizations shall be registered to assist in ensuring proper levels of protection consistent with Departmental standards to prevent unacceptable, adverse impact on national security or on the health and safety of DOE and contractor employees, the public, or the environment.

   c. If no need exists for a contractor's office locations to receive, process, reproduce, store, transmit, or handle classified information or nuclear material, but access authorizations are required for the contractor to perform the work within DOE-approved facilities, the contractor (identified as a non-possessing facility) must be registered. As used in this Contractor Requirements Document, the term facility clearance refers to both possessing and non-possessing facilities.

   d. Facility clearance shall be based upon a determination that satisfactory safeguards and security can be afforded the safeguards and security activities. The determination of a valid facility clearance shall be based upon an approved safeguards and security plan, results of surveys, and a favorable FOCI determination, as appropriate.

   e. Approval for other Federal agency safeguards and security activities to be conducted at Department-owned or -operated facilities shall be based on a determination that the safeguards and security measures to be provided are consistent with Departmental policy.

   f. Facility clearance for work-for-others safeguards and security activities at other than Department-owned or -operated facilities that are channeled through a Departmental entity shall be based on the validation of the other agency's facility clearance.

      (1) Before commencement of non-DOE funded work, conduct, as required by DOE 5650.2B, IDENTIFICATION OF CLASSIFIED INFORMATION, of 12-31-91, a review of the

work request and certify that the sponsoring organization has either provided the appropriate classification guidance or has stated in writing that the non-DOE funded work will not entail classified activities.

(2) Ensure, prior to commencement of the non-DOE funded work involving access authorization, that safeguards and security activities have been recorded as security interests on DOE F 5634.2, "Contract Security Classification Specification," or DD F 254, "Contract Security Classification Specification."

(3) Ensure, before acceptance of any work for another Federal agency, that appropriate reimbursement for safeguards and security costs is negotiated.

3. REQUIREMENTS: FACILITY CLEARANCES.

a. Granting Approval. Approval of a facility is based on the following.

(1) A favorable foreign ownership, control or influence (FOCI) determination, in accordance with Chapter VI of this contractor requirements document.

(2) A Facility National Agency Check, which has been requested or completed on those facilities that do not possess a Department of Defense (DOD) facility clearance, in accordance with this chapter.

(3) For contractors, contract(s) containing appropriate security clauses.

(4) Approved safeguards and security plans, as appropriate.

(5) If nuclear materials are involved, an established Reporting Identification Symbol code for Nuclear Materials Management and Safeguards System reporting.

(6) For the facility to possess classified matter, nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, or over $5,000,000 of DOE property, not including facilities or land values, at its location, an initial survey or other survey resulting in a report that comprehensively addresses the security interest, conducted no more than 6 months before the facility clearance date, with a composite facility rating of satisfactory.

(7) Appointment of a Facility Security Officer and, if applicable, Materials Control and Accountability Representative. The Facility Security Officer must possess a personnel clearance equivalent with the facility clearance.

(8) Access authorizations for appropriate personnel. Key management personnel must be determined case by case. Key management personnel must be cleared to the level of the facility clearance. Other officials, to be determined by the Lead Responsible Office, must

possess appropriate access authorization for classified information or special nuclear materials.

b. Accepting a Contractor's Existing Federal Agency Facility Clearance. A contractor facility holding facility clearance from another Federal agency may be approved by DOE for processing, using, or storing classified matter, contingent upon the actions required by DOE O 470.1.

4. REQUIREMENTS: FACILITY DATA AND APPROVAL RECORD. A DOE F 5634.3, "Facility Data and Approval Record," shall be prepared by the procurement request originator, who forwards the completed form, through their own safeguards and security organization, to the cognizant Departmental safeguards and security organization.

a. If a subcontract is established between a DOE prime contractor and another contractor for work involving access authorizations, classified matter or nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat, it is the responsibility of the prime contractor to ensure the proper preparation of a DOE F 5634.3.

b. The prime contractor is responsible for forwarding information on the DOE F 5634.3 requiring updating to the cognizant Departmental safeguards and security organization.

5. REQUIREMENTS: CONTRACT SECURITY CLASSIFICATION SPECIFICATION.

a. New Activity. If a new activity for work involving access authorizations is being considered, the DOE F 5634.2 (or the DD F 254, "Contract Security Classification Specification") must be submitted by the procurement request originator to the Contracting Officer's Representative.

b. Preparation. A DOE F 5634.2 shall be initially prepared by the procurement request originator, who forwards the completed form to the cognizant Departmental Element Safeguards and Security organization. If a DD Form 254, "Contract Security Classification Specification" has been used by the agency sponsoring the activity, it shall be annotated with the facility code and submitted instead of the DOE F 5634.2.

# CHAPTER VI

## FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE PROGRAM

1. APPLICABILITY. Foreign ownership, control, or influence (FOCI) determinations are required of the following.

   a. Contractors, which include any industrial, educational, commercial, or other entity, grantee, or licensee, including an individual, that has executed an agreement with the Federal Government for the purpose of performing under a contract, license, or other arrangement that requires access authorizations. This includes subcontractors of any tier, consultants, agents, grantees, and cooperative agreement participants.

   b. All tier parents, if the contractor is owned or controlled by another firm(s).

2. REQUIREMENTS.

   a. A facility clearance, which includes a FOCI determination, can only be requested for the successful offeror/bidder if insufficient lead time is expected between selection and contract award to allow deferral of the review.

   b. Contractors shall submit to the Contracting Officer information and documentation that define the extent and nature of any foreign ownership, control, or influence over the contractor and, if applicable, tier parents.

   c. Contractors and any tier parents, subject to the FOCI requirements must submit the following to the Lead Responsible Office:

      (1) Written notification of a change in the extent and nature of FOCI that affects the information in the FOCI representation and certification.

      (2) Complete, current, and accurate information, certifications, and explanatory documentation that define the extent and nature of any relevant FOCI whenever:

         (a) there is any change in ownership or control,

         (b) 5 years have elapsed since the previously provided FOCI representation and certification were executed, or

         (c) the Lead Responsible Office advises that it considers that a relevant change in the nature of the FOCI has occurred.

(3) Written notification of anticipated changes that include, but are not limited to, the following:

(a) action to terminate the contractor organization or any of its parents for any reason;

(b) imminent adjudication of or reorganization in bankruptcy of the contractor organization or any tier parents;

(c) discussions or consultations with foreign interests that may reasonably be expected to lead to the introduction or increase of FOCI; or

(d) negotiations for the sale of securities to a foreign interest that may lead to the introduction or increase of FOCI.

3. REQUIREMENTS: REPORTING SIGNIFICANT CHANGES. When a changes in the extent and nature of FOCI that would affect the information in a contractor's and/or any tier parents' most recent DOE FOCI submission(s) has occurred, the contractor/parent shall immediately provide written notification and supporting documentation relevant to the changes to the DOE Lead Responsible Office. A significant FOCI increase/change that warrants processing of the contractor/parent for a new FOCI determination includes, but is not necessarily limited to, the following.

a. A new threshold or factor that did not exist when the previous determination was made (e.g., a "no" answer changes to a "yes" answer), and any additional factors associated with the questions on the FOCI representation and certification.

b. A previously reported threshold or factor that was favorably evaluated by the Lead Responsible Office has increased to a level requiring a determination by the Office of Safeguards and Security.

c. A previously reported financial threshold or factor that was favorably evaluated has increased by 5 percent or more; or a shift has occurred of 5 percent or more by country location or end user (i.e., for revenue) or lenders (i.e., indebtedness).

d. A previously reported foreign ownership threshold or factor that was favorably evaluated by the Office of Safeguards and Security has increased to the extent that a method of negation or reduction is necessary.

e. Any changes in the ownership or control of the contractor and/or any tier parents.

4. REQUIREMENTS: METHODS TO NEGATE OR REDUCE UNACCEPTABLE FOCI. The affected U.S. organization(s), or its legal representatives may propose a plan to negate or reduce unacceptable FOCI, but the primary responsibility for approving such a plan rests with the Office of Safeguards and Security. A plan may consist of one or more of the insulating measures identified in DOE O 470.1, Chapter VI.

5. REQUIREMENTS: ANNUAL CERTIFICATION.

a. At the end of each year of operation, the Trustees, Proxy Holders, or other principals, as appropriate, shall submit to the Lead Responsible Office an annual implementation and compliance report. Failure of the cleared U.S. organization to ensure compliance with the terms of the applicable security arrangement may result in the organization's facility clearance being suspended pending resolution of the FOCI.

b. Each contractor holding a facility clearance shall certify annually to the Lead Responsible Office that (i) no significant changes have occurred in the extent and nature of FOCI that would affect the organization’s answer to the questions provided in its FOCI representations; (ii) no changes have occurred in the organization’s ownership; and (iii) no changes have occurred in the organization’s officers, directors, and executive personnel.

c. When the contractor is controlled by parent organizations that have been excluded, the contractor must also provide annually to the Lead Responsible Office written certification from an authorized official from each such excluded parent that (i) no significant changes have occurred in the extent and nature of FOCI that would affect the organization’s answer to the questions provided in its FOCI representations; (ii) no changes have occurred in the organization’s ownership; and (iii) no changes have occurred in the organization’s officers, directors, and executive personnel.

# CHAPTER VII

## INCIDENTS OF SAFEGUARDS AND SECURITY CONCERN

1. APPLICABILITY.

   a. When an inquiry establishes credible information that fraud, waste and/or abuse has occurred, which does not involve a national security interest has occurred, the Office of the Inspector General shall be notified for information and/or action.

   b. When an inquiry establishes that a potential compromise or unauthorized disclosure of classified information, the applicable provision of DOE O 471.2, INFORMATION SECURITY PROGRAM, shall be followed.

   c. Employees with information indicating possible fraud, waste, abuse, or other forms of wrongdoing in the Department's programs or operations shall inform the Inspector General immediately upon obtaining such information.

2. REQUIREMENTS.

   a. Loss, compromise, or unauthorized disclosure of classified information, and alleged or suspected violations of laws pertaining to safeguards and security shall be reported promptly through the appropriate DOE Element to the Office of Safeguards and Security, Secretarial Officer, and when appropriate, the local Federal Bureau of Investigation office.

   b. Unclassified reports and notifications of safeguards and security incidents shall be made in accordance with DOE O 232.1, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION; and DOE O 471.2, INFORMATION SECURITY PROGRAM. Reports which contain classified information shall contain all of the information required by DOE O 232.1, but shall not be entered on the Occurrence Reporting and Processing System. Classified reports shall be sent by approved methods for transmitting classified information. Reporting intervals for incidents of safeguards and security concern must be in accordance with DOE O 232.1.

   c. Federal Bureau of Investigation personnel shall be admitted to areas and afforded access to Restricted Data or other classified information as necessary for them to perform their duties. Such personnel shall be provided escort, as necessary, for safety reasons or to facilitate the investigative progress.

   d. When Federal Bureau of Investigation personnel are given access to classified information, they will be immediately advised of the classification and the category of the information. Appropriate document and data classification, marking information, and protection and control requirements shall be made available to them through local liaison channels.

# CHAPTER VIII

## CONTROL OF CLASSIFIED VISITS PROGRAM

1. APPLICABILITY. The requirements in this chapter apply to contractor personnel who visit DOE facilities that entail access to classified information.

2. REQUIREMENTS: CLASSIFIED VISIT PROCEDURES. A contractor's basic procedures for the control of all classified visits to DOE facilities shall ensure the following.

   a. Verification of the identity, access authorization (security clearance), and need-to-know of the visitor.

   b. Observance of limitations on access to classified information or facilities.

   c. Timely notification (10 days) of visits.

   d. Prompt transmittal of "Request for Visit or Access Approval" (DOE F 5631.20), when applicable. (This form is no longer required for DOE and DOE contractor employees who visit DOE facilities. These employees may use their DOE picture identification badge as evidence of a DOE access authorization. However, DOE F 5631.20 is still required for programmatic approval for sigma access and for employees of other Federal agencies who visit DOE facilities.)

   e. Timely notification to those concerned for approval of access to weapon data (classified Secret or Top Secret), Top Secret information (nonweapon data), sensitive nuclear materials production information, atomic vapor laser isotope separation technology, uranium enrichment technology, or facilities specifically designated by Headquarters Elements.

   f. Use of continuing visitor access approval as necessary for individuals who visit DOE facilities frequently. This approval cannot exceed a period of 1 year, but the approval may be renewed annually, if necessary.

   g. Operational approval of visits.

   h. Maintenance of records of all classified visits by non-DOE personnel and foreign nationals.

   i. Referral to the Director of Public and Consumer Affairs of any nonroutine, written, or visual material proposed for public release resulting from visits.

3. REQUIREMENTS: CLASSIFIED VISITS BY DOE EMPLOYEES, CONTRACTORS AND SUBCONTRACTORS.

a. The visitor is responsible for making administrative arrangements and obtaining approval from the Field Element or Secretarial Officer, as appropriate. (The authority granting such approval is responsible for informing the office to be visited.)

b. When the amount of visitor traffic between DOE contractor or subcontractor facilities due to mutual program interests is significant, contractors or subcontractors may be authorized, subject to the limitations in subparagraph c below, to arrange for the visits without obtaining DOE approval if such authorization will be advantageous to DOE.

c. The following procedures are required when access to weapon data (classified Secret or Top Secret), Top Secret information (nonweapon data), sensitive nuclear materials production information, atomic vapor laser isotope separation technology, uranium enrichment technology, or specific facilities designated by Headquarters Elements having program direction is required.

(1) A determination of the need for access shall be made by the DOE official sponsoring the visit.

(2) Approval of the access during visits under the auspices of a Headquarters Element should be obtained from the Headquarters Element exercising jurisdiction over the facility or office to be visited.

(3) Approval of this access during visits under the auspices of Field Elements shall be obtained from the responsible Field Element for field visits, and for visits to Headquarters, from the organization being visited.

4. REQUIREMENTS: VISITS TO DEPARTMENT OF DEFENSE AND NATIONAL AERONAUTICS AND SPACE ADMINISTRATION FACILITIES.

a. A DOE F 5631.20 shall be forwarded directly by contractors, through DOE Elements, to the commanding officer or the director of the facility after first verifying the visitor's clearance at the DOE Element.

b. DOE Top Secret approvals shall be specifically certified in the event access to Top Secret information is required.

c. Any exchange of Restricted Data occurring during the course of the visit shall be accomplished as stated in paragraph 7 below.

5. REQUIREMENTS: RESTRICTED DATA VISITS BY NUCLEAR REGULATORY COMMISSION EMPLOYEES.

a. Visits to DOE facilities by Nuclear Regulatory Commission employees, consultants, contractors, or subcontractors who require access to weapon data, sensitive nuclear materials

production information, atomic vapor laser isotope separation technology, or uranium enrichment technology, or entry into a DOE classified weapon or production facility shall:

(1) be arranged through the respective Headquarters Element that will coordinate the visits;

(2) if to classified weapon or production facilities, have prior approval of the Assistant Secretary for Defense Programs; and

(3) have DOE F 5631.20 or the Nuclear Regulatory Commission equivalent with necessary clearances certified by the Director of Security, Nuclear Regulatory Commission.

b. Visits involving access to other Restricted Data not requiring prior approval from the appropriate Headquarters official exercising jurisdiction over the facility or office to be visited may be arranged directly by Nuclear Regulatory Commission with the cognizant DOE Element, provided this procedure does not conflict with the existing visitor control procedures of the division or office having program responsibility. A DOE F 5631.20 or Nuclear Regulatory Commission equivalent is required.

c. The Nuclear Regulatory Commission identification badge shall not be used as authority for visits in lieu of the aforementioned specific visit approval arrangements.

6. REQUIREMENTS: RESTRICTED DATA VISITS BY DEPARTMENT OF DEFENSE AND NATIONAL AERONAUTICS AND SPACE ADMINISTRATION EMPLOYEES.

a. Access to Restricted Data is contingent upon submission of a DOE F 5631.20, National Aeronautics and Space Administration Form-405, "Request for Access Approval," or a memorandum or electronic message signed by or in the name of the certifying official. The request shall be forwarded for approval or other action to the DOE official with jurisdiction over the information to which access is desired.

b. The request for access shall include the following:

(1) Name(s) of person(s) and organization represented (if not Armed Forces, relationship to the Department of Defense or National Aeronautics and Space Administration).

(2) Information to which access is desired. Access to critical nuclear weapon design information must be specified when it is required.

(3) The security clearance or access authorization status of each person.

(4) Certification that the person needs the access in the performance of duty.

(5) Anticipated date of visit and names of persons to be visited, as appropriate (if a conference is involved, the date, place, and sponsor of the conference shall be specified).

(6) Statement of determination that permitting the person(s) access will not endanger the common defense and security.

(7) Citizenship and date of birth.

(8) For requests from National Aeronautics and Space Administration, a certification that the matter to which access is desired relates to "aeronautical and space activities."

c. The approving official must possess or have been delegated the authority to approve such access. The approving official must satisfy himself/herself:

(1) as to person's identity,

(2) that the person's clearance or access authorization is at least equal to the classification of the information to which access is desired.

d. Access to Restricted Data in the custody of DOE contractors and subcontractors may be authorized by Heads of DOE Elements in accordance with the following:

(1) The person's identity has been established.

(2) The person's clearance or access authorization, as indicated in the request, is at least equal to the classification of the information to which access is desired.

(3) Access to certain programs or information is handled in accordance with the following:

(a) Weapons Production Programs. For access to weapons programs, nuclear materials production facilities, or sensitive nuclear materials production information, the requests shall be referred to the Assistant Secretary for Defense Program.

(b) Uranium Enrichment. For access to uranium enrichment plants or facilities engaged in uranium enrichment technology development, including advanced isotope separation technology, the request shall be referred to the Office of Uranium Programs.

(c) Naval Nuclear Propulsion Information. When access is desired to Naval Nuclear Propulsion Information, the request shall be referred to the Office of Naval Reactors.

e. Control of access by members of the Armed Services or Department of Defense or National Aeronautics and Space Administration personnel or contractors to Restricted Data in the custody of another Federal agency is the responsibility of the appropriate official or his/her

designee named in DOE O 470.1. Federal officials named are responsible for maintaining a central index to record access approvals.

7. REQUIREMENTS: OTHER CLASSIFIED VISITS BY DEPARTMENT OF DEFENSE AND NATIONAL AERONAUTICS AND SPACE ADMINISTRATION EMPLOYEES .

   a. Requests for such visits to contractor and subcontractor facilities are approved by Heads of Field Elements or, in the case of Headquarters Elements, by the head of the element concerned after assuring that such visitor possesses appropriate military or National Aeronautics and Space Administration security clearance and requires the information in the performance of his/her duties.

   b. Certification of security clearance may be made by memorandum, electronic message, DOE F 5631.20, or National Aeronautics and Space Administration Form 405.

8. REQUIREMENTS: CLASSIFIED VISITS BY EMPLOYEES OF OTHER FEDERAL AGENCIES.

   a. Requests for visits to DOE facilities by employees, contractors, or subcontractors of Federal agencies other than the Department of Defense, National Aeronautics and Space Administration, or Nuclear Regulatory Commission are approved by the Field Elements or, for Headquarters, by the organization concerned.

   b. Restricted Data may not be exchanged with persons in this category unless they possess appropriate DOE access authorization.

   c. Classified information other than Restricted Data may be exchanged with such individuals if they possess Q or L access authorizations or security clearances under the provisions of Executive Order 10450, "Security Requirements for Government Employment," and require the information in the performance of their duties.

9. REQUIREMENTS: CONGRESSIONAL AND STATE CLASSIFIED VISITS.

   a. Requests for visits to DOE, contractor, or subcontractor facilities by members or employees of Congress or congressional committees and by Governors or their staffs may be approved by Heads of DOE Elements provided the following are established.

      (1) The visitors' identities.

      (2) Access authorization or security clearance.

      (3) "Need-to-know."

b. The Assistant Secretary for Congressional and Intergovernmental Affairs shall be advised of requests and action taken on the requests for such visits.

10. REQUIREMENTS: EMERGENCY VISITS TO CLASSIFIED AREAS AND FACILITIES.

a. In an emergency, requests for visit approval may be made by telephone or electronic message.

b. Telephonic requests must be confirmed by memorandum or electronic message.

11. REQUIREMENTS: CLASSIFIED VISITS BY FOREIGN NATIONALS TO DOE FACILITIES.

a. Visits by foreign nationals possessing Department of Defense or National Aeronautics and Space Administration security clearances will be arranged in accordance with paragraph 6 above.

b. Visits by foreign nationals possessing security clearances granted by Federal agencies other than the DOE, Department of Defense, or National Aeronautics and Space Administration shall be arranged in accordance with paragraph 7 above.

c. Visits by foreign nationals who are sponsored by a foreign government shall be arranged as follows.

(1) If the visit is in connection with the military application of atomic energy under sections 144b and c(1) and 91c(1) or (4) of the Atomic Energy Act of 1954, as amended, the Assistant Secretary for Defense Programs shall make all arrangements for the visit, including appropriate approvals and security assurances.

(2) If the visit is to the Office of Declassification in connection with the information classification program under DOE 5650.2B, IDENTIFICATION OF CLASSIFIED INFORMATION, of 12-31-91, the Director of Declassification shall make arrangements for the visit, including appropriate approvals and security assurances.

(3) If the visit is not in connection with programs covered in the above paragraphs, the Deputy Assistant Secretary for International Energy Policy shall arrange for the visit in concert with the appropriate Headquarters staff other than those listed above, and shall coordinate with the Director of Safeguards and Security for the necessary security assurances.

(4) If the visit is in connection with naval nuclear propulsion matters, the Director of Naval Reactors shall make arrangements for the visit, and shall have the Director of Safeguards and Security obtain the necessary security assurances.

(5) Security assurances received under the above paragraphs shall be retained for 5 years.

# CHAPTER IX

## SURVEY PROGRAM

1. APPLICABILITY. The Survey Program applies to all facilities that are eligible to have access to, use, store, or transmit nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat and/or classified information, that require access authorizations, or that possess over $5,000,000 of DOE property, exclusive of facilities and land values.

2. REQUIREMENTS: CORRECTIVE ACTIONS.

   a. When a survey contains findings, the surveyed organization shall submit a response identifying corrective action(s) for each finding to the Responsible and Surveying Offices no later than 30 working days after the formal receipt of findings. The corrective action(s) should be based on documented root cause analysis, risk assessment, and cost-benefit analysis.

   b. Contractors shall provide quarterly reports of corrective action(s) for each finding to the Responsible and Surveying Offices.

# CHAPTER X

## SELF-ASSESSMENT PROGRAM

1. APPLICABILITY. This program applies to contractor facilities for which a DOE F 5634.3, "Facility Data and Approval Record," is recorded. The level of detail of the self-assessment may be specified by the Lead Responsible Office.

2. REQUIREMENTS.

   a. Self-assessment programs shall be conducted and documented for all cleared facilities. The self-assessment program shall:

      (1) include reviews of all applicable DOE F 5634.1, "Safeguards and Security Survey Report," topical and subtopical areas of the facility's safeguards and security program/system;

      (2) be conducted between the periodic surveys conducted by the Surveying Office; and

      (3) be conducted using personnel knowledgeable of the programmatic or topical area.

   b. Self-assessment reports shall:

      (1) address reviewed topical areas;

      (2) be used as organizational management tools/aids in determining the status of safeguards and security performance and compliance with applicable safeguards and security order requirements;

      (3) be available for review by the Surveying Office during surveys; and

      (4) list findings resulting from self-assessment activities.

   c. Findings resulting from self-assessments shall be processed as follows:

      (1) Reviewed during the surveys by the Surveying Office.

      (2) Addressed by facility/organization management through a documented corrective action plan.

      (3) Reviewed and the status of findings tracked until closed.

      (4) Reported to the Lead Responsible Office if:

(a) a vulnerability to national security, classified information, nuclear materials, or Departmental property results, or may result, in a significant anomaly that could have significant programmatic impact or embarrass the Department; or

(b) the self-assessment is used to extend the Surveying Office's periodic survey frequency.

(5) be documented in survey reports when deficiencies still exist and have not been adequately addressed.

# DEVIATION REQUEST FORMAT

1. Date. Date the request is signed by the requesting official.

2. Request Number. Alphanumeric identifier beginning with "OSS," followed by the routing symbol used in the DOE National Telephone Directory, followed by the last two digits of the year in the request's date, followed by the three-digit number that is next in the sequence of requests from that Field Element in that calendar year. For example, the third request from Albuquerque Operations Office during 1995 would be OSS-AL-95-003.

3. Directive Citation. Title and date of the directive from which a deviation is being requested with a citation (paragraph or other provision) and summary of the directive's requirement.

4. Impacted Entity. Identification of the specific facility (Safeguards and Security Information Management Systems facility code number), process, procedure, system, etc.

5. Deviation Justification. Specific description of the deviation and the associated reason or rationale for the deviation request. A description of the relationship of the subject of the deviation request to other safeguards and security interests shall be included if they are significantly affected.

6. Protection Measures. Description of the current measure(s) used for protection and an evaluation of the effectiveness of such measure(s); description of alternate/compensatory measure(s) or level(s) of protection to be provided as an alternative to the Order requirement(s).

7. Duration. Expected duration of the condition for which the deviation is requested, including milestones for correcting, alleviating, or eliminating the deviant condition, if applicable. (Note: Waivers cannot be for more than 2 years; exceptions cannot be for more than 3 years.)

8. Risks. Evaluation of the risk associated with the deviation, if approved. Results of vulnerability analyses and performance tests conducted on proposed alternative(s) shall be included.

9. Signature. Requesting official's signature.